NGINX*Conf 2018

The official event for all things NGINX

NGINX* Transport Layer Security (TLS) and Payload Compression Accelerated with Intel® QuickAssist Technology

Gordon McFadden
Intel Corporation

Legal Disclaimers

- You may not use or facilitate the use of this document in connection with any infringement or other legal analysis concerning Intel products described herein. You agree to grant Intel a non-exclusive, royalty-free license to any patent claim thereafter drafted which includes subject matter disclosed herein.
- No license (express or implied, by estoppel or otherwise) to any intellectual property rights is granted by this document.
- All information provided here is subject to change without notice. Contact your Intel representative to obtain the latest Intel product specifications and roadmaps.
- The products described may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.
- Copies of documents which have an order number and are referenced in this document may be obtained by calling 1-800-548-4725 or by visiting: http://www.intel.com/design/literature.htm
- Results have been estimated or simulated using internal Intel analysis or architecture simulation or modeling, and provided to you for informational purposes. Any differences in your system hardware, software or configuration may affect your actual performance.
- No computer system can be absolutely secure.
- Intel, Xeon, Intel® QuickAssist Technology, and the Intel logo are trademarks of Intel Corporation in the U.S. and/or other countries.
- *Other names and brands may be claimed as the property of others.
- Copyright © 2018, Intel Corporation. All rights reserved.

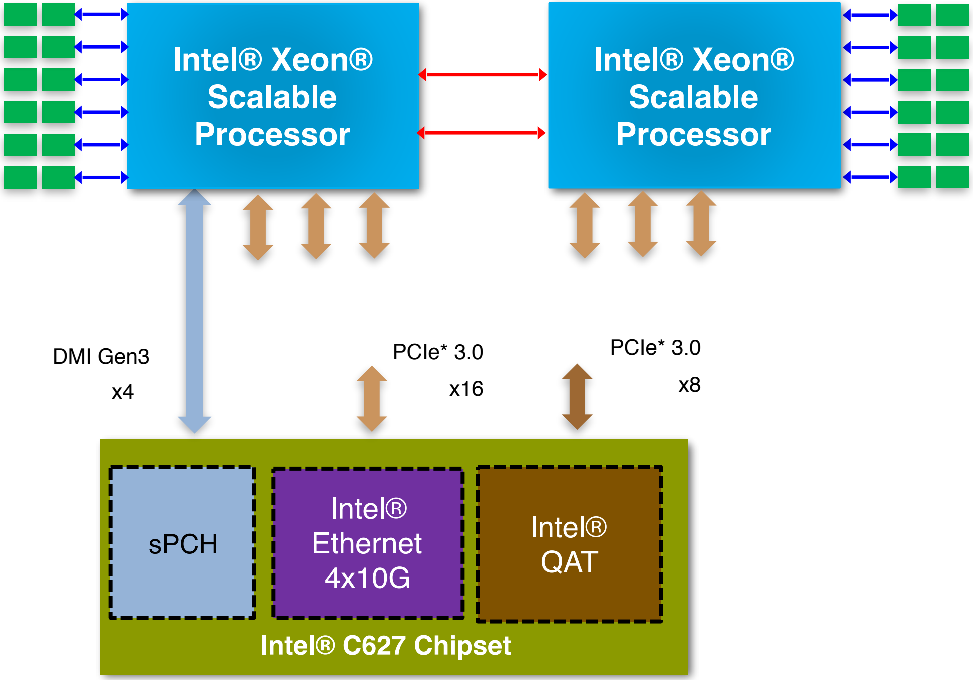
Agenda

1
- Introduction to Intel® QuickAssist Technology (Intel® QAT) Hardware and Software

2
- NGINX* configuration file for Intel® QAT SSL and Compression

3
- Results

Gen 2 Intel® QAT as a Platform Component



Intel® C627 Chipset

Three Separate Subsystems

- Server class Platform Control Hub (PCH) via Direct Media Interface (DMI) Gen 3 x4
- I/O (4x10G with iWARP RDMA)
- Intel® QAT
  - Crypto and Compression Hardware Acceleration
  - >100 Gbs Bulk Crypto
  - 100 kops RSA 2 k Decrypt
  - 68 Gbs Verified Compression
  - 160 Gbs Decompression
  - Supports SR-IOV with 3 PF, 48 Trusted VFs

    (Acceleration and I/O via PCIe* x16 and/or x8 Gen 3)

Supports multiple configurations

- Down on Motherboard as PCH, Ethernet and/or Intel® QAT Acceleration

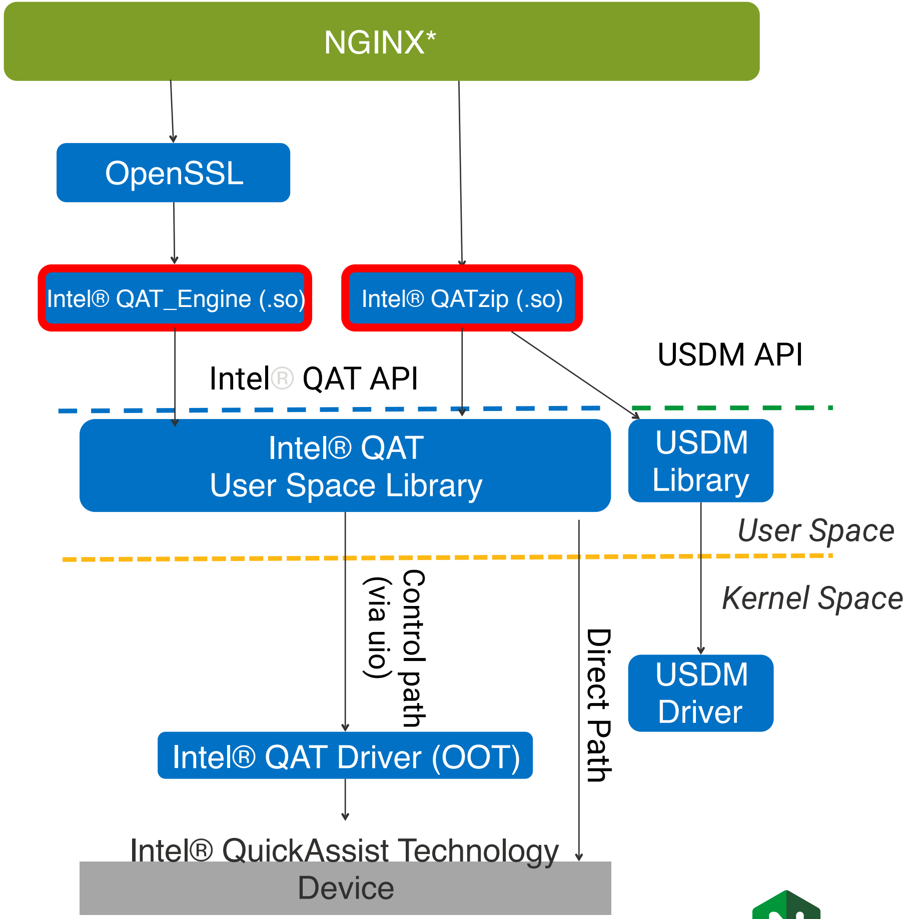
  and/or

- PCIe* add-in card for Ethernet and/or QAT Acceleration

NOTE: Separate power planes and Connectivity for power optimized configurations

Software Stack

- Intel® QAT zip is a high performance user space library designed for environments requiring both highly threaded processes and/or many processes
- Intel® QAT user space library provides access to both the Intel® QAT out-of-tree driver and directly to the Intel® QAT device via memory mapped address space
- Out-of-tree driver is a superset of the in-tree drive
  - User space applications via Intel® QAT API, via “direct model”, for instance, queues are mapped to user space (for performance)
- User-Space DMA-able Memory Library Driver also supplied
- QAT_Engine is a .so that plugs into the engine framework of openSSL, providing crypto services from Intel® QAT



Nginx Configuration File

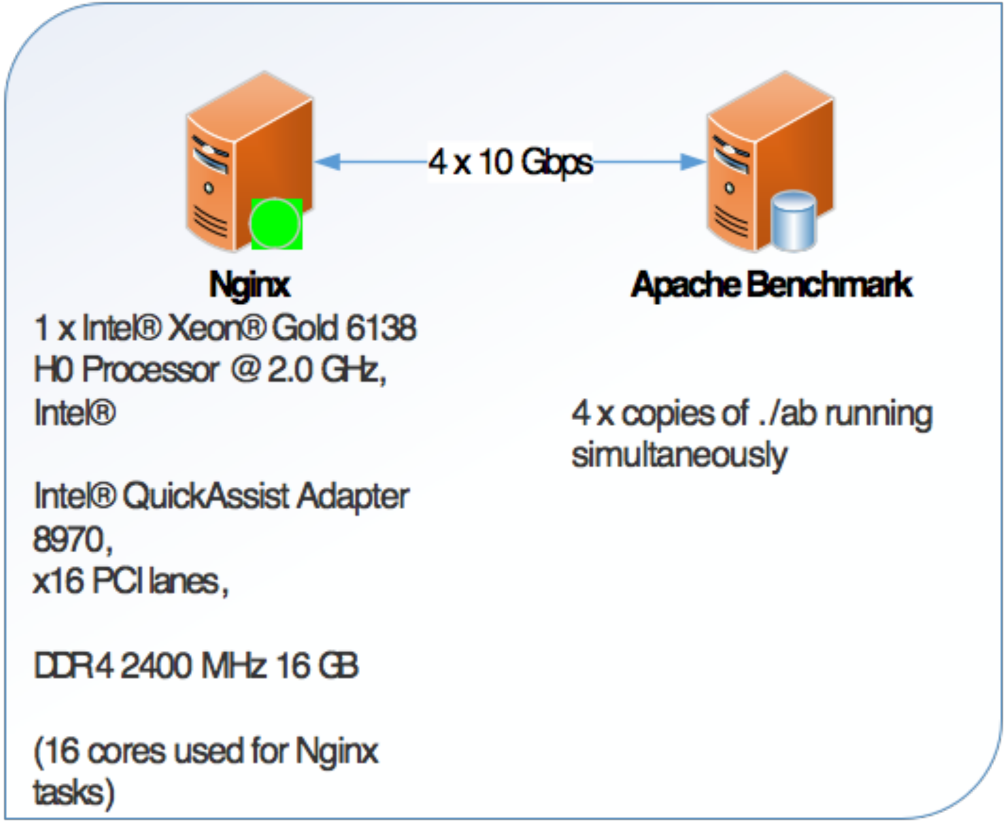
```
load_module modules/ngx_http_qatzip_filter_module.so;
        qatzip on;
        gzip_proxied any;
        qatzip_min_length 128;
        qatzip_comp_level 1;
        qatzip_buffers 16 16k;
        qatzip_types text/css text/javascript text/xml text/plain text/x-component
application/javascript application/json application/xml application/rss+xml font/
truetype font/opentype application/vnd.ms-fontobject image/svg+xml application/octet-
stream image/jpeg;
        qatzip_chunk_size 64k;
        qatzip_stream_size 2092032;
        qatzip_sw_threshold 2k
```

Nginx Configuration File (Cont.)

```
load_module modules/ngx_ssl_engine_qat_module.so;

ssl_engine{
      use_engine qat;
      default_algorithms ALL;
      qat_engine{
            qat_offload_mode async;
            qat_notify_mode poll;
            qat_poll_mode heuristic;
}}
```

Performance Test Setup



4 x 10 Gbps

Nginx

1 x Intel® Xeon® Gold 6138 H0 Processor @ 2.0 GHz, Intel®

Intel® QuickAssist Adapter 8970,
x16 PCI lanes,

DDR4 2400 MHz 16 GB

(16 cores used for Nginx tasks)

Apache Benchmark

4 x copies of ./ab running simultaneously

Performance Test Input

Four files:

- front pages from English language news sites

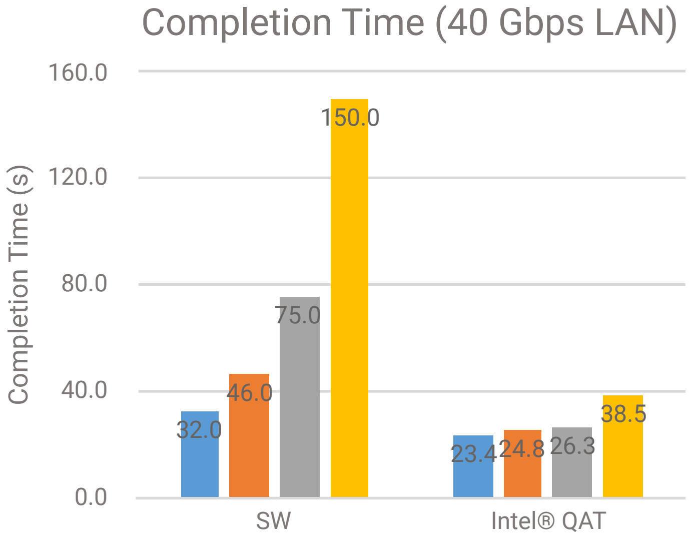
ABC News*	First 5,441 bytes
Cable Network News* (CNN)	137,231 bytes
Times of India*	372,028 bytes
Shanghai Daily*	64,137 bytes

Tests ran concurrent with four copies of Apache Benchmark (ab).

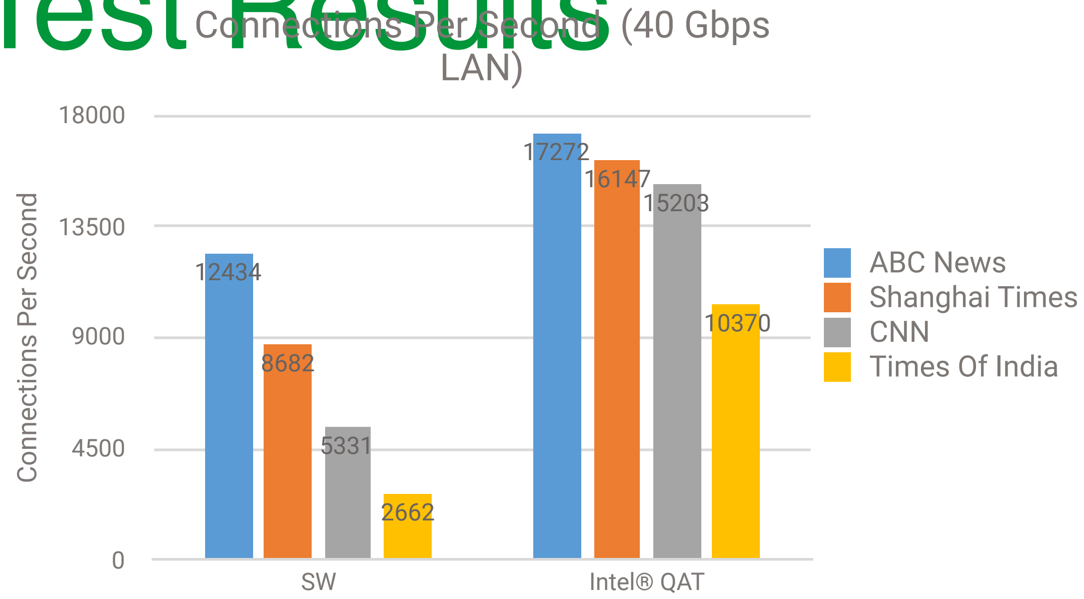
Example:

```
ab -n 100000 -c 100 -Z AES128-SHA -f TLS1.2 -H 'Accept Encoding:gzip,deflate'  https://
172.16.1.1:4400/<name_of_file>
```

Performance Test Results



Completion Time (40 Gbps LAN)



Connections Per Second (40 Gbps LAN)

1 x Intel® Xeon® Gold 6138P Processor @ 2.0 GHz, Intel® QuickAssist Adapter 8970, x16 PCI lanes, DDR4 2400 MHz 16 GB

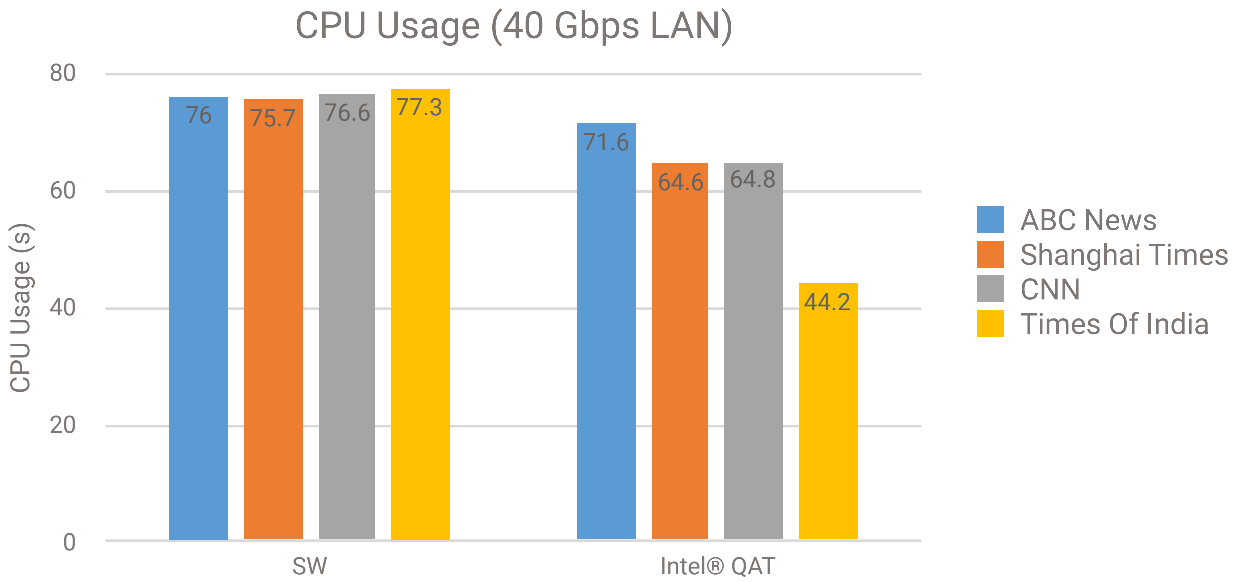
16 cores used for Nginx* tasks

1. Results have been estimated based on internal Intel analysis and are provided for informational purposes only. Any difference in system hardware or software design or configuration may affect actual performance.
2. All products, platforms, dates, features, and figures specified are preliminary based on current expectations and are subject to change without notice.
3. Software and workloads used in performance tests may have been optimized for performance only on Intel microprocessors.

   Performance tests, such as SYSmark* and MobileMark*, are measured using specific computer systems, components, software, operations and functions. Any change to any of those factors may cause the results to vary. You should consult other information and performance tests to assist you in fully evaluating your contemplated purchases, including the performance of that product when combined with other products. For more complete information visit www.intel.com/benchmarks.

   Configurations: See slides 9 and 10 for configurations. Testing performed by Intel.
4. Performance results are based on testing as of September 25, 2018 and may not reflect all publicly available security updates. See configuration disclosure for details. No component or product can be absolutely secure.

Performance Test Results



1 x Intel® Xeon® Gold 6138P Processor @ 2.0 GHz, Intel® QuickAssist Adapter 8970, x16 PCI lanes, DDR4 2400 MHz 16 GB

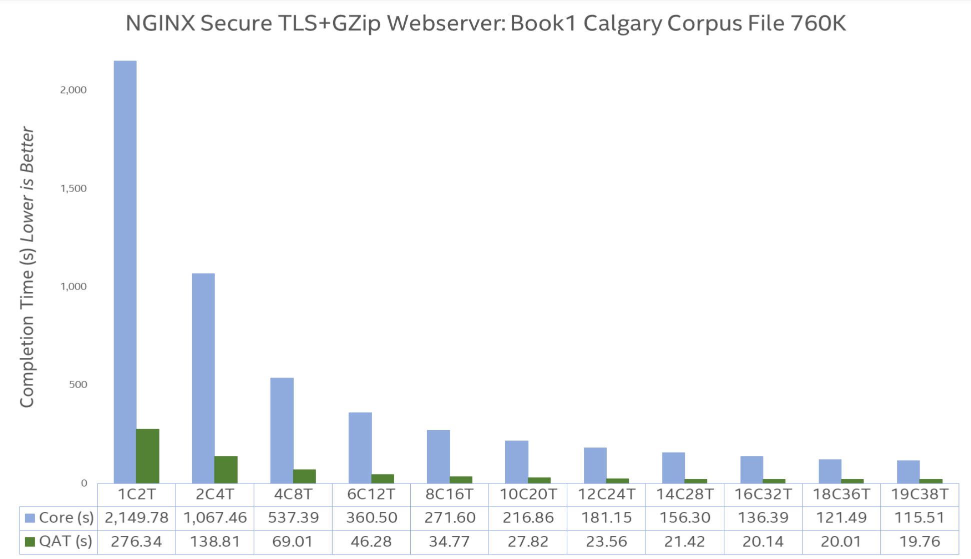
16 cores used for Nginx* tasks

1. Results have been estimated based on internal Intel analysis and are provided for informational purposes only. Any difference in system hardware or software design or configuration may affect actual performance.
2. All products, platforms, dates, features, and figures specified are preliminary based on current expectations and are subject to change without notice.
3. Software and workloads used in performance tests may have been optimized for performance only on Intel microprocessors.

   Performance tests, such as SYSmark* and MobileMark*, are measured using specific computer systems, components, software, operations and functions. Any change to any of those factors may cause the results to vary. You should consult other information and performance tests to assist you in fully evaluating your contemplated purchases, including the performance of that product when combined with other products. For more complete information visit www.intel.com/benchmarks.

   Configurations: See slides 9 and 10 for configurations. Testing performed by Intel.
4. Performance results are based on testing as of September 25, 2018 and may not reflect all publicly available security updates. See configuration disclosure for details. No component or product can be absolutely secure.

Core Scaling Results


NGINX Secure TLS+GZip Webserver: Book1 Calgary Corpus File 760K

	1C2T	2C4T	4C8T	6C12T	8C16T	10C20T	12C24T	14C28T	16C32T	18C36T	19C38T
■ Core (s)	2,149.78	1,067.46	537.39	360.50	271.60	216.86	181.15	156.30	136.39	121.49	115.51
■ QAT (s)	276.34	138.81	69.01	46.28	34.77	27.82	23.56	21.42	20.14	20.01	19.76

1 x Intel® Xeon® Gold 6138P Processor @ 2.0 GHz, Intel® QuickAssist Adapter 8970, x16 PCI lanes, DDR4 2400 MHz 16 GB

16 cores used for Nginx* tasks

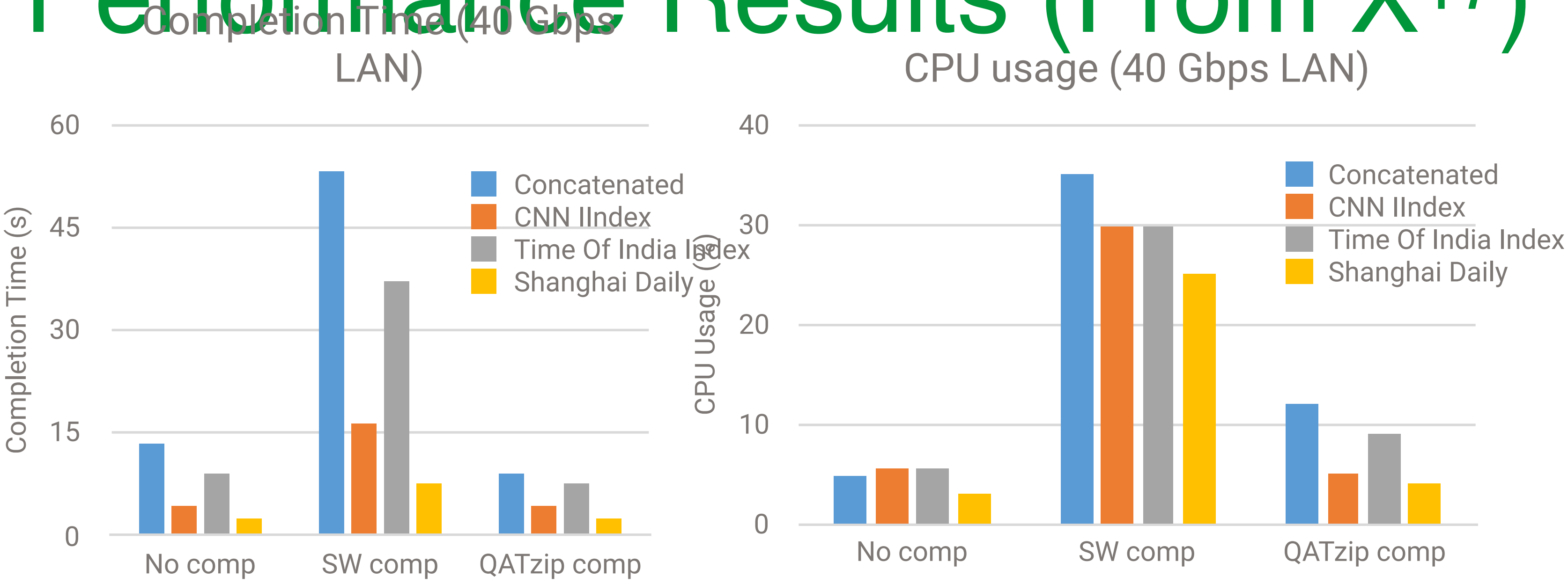
1. Results have been estimated based on internal Intel analysis and are provided for informational purposes only. Any difference in system hardware or software design or configuration may affect actual performance.
2. All products, platforms, dates, features, and figures specified are preliminary based on current expectations and are subject to change without notice.
3. Software and workloads used in performance tests may have been optimized for performance only on Intel microprocessors.

   Performance tests, such as SYSmark* and MobileMark*, are measured using specific computer systems, components, software, operations and functions. Any change to any of those factors may cause the results to vary. You should consult other information and performance tests to assist you in fully evaluating your contemplated purchases, including the performance of that product when combined with other products.   For more complete information visit www.intel.com/benchmarks.

   Configurations: See slides 9 and 10 for configurations. Testing performed by Intel.
4. Performance results are based on testing as of September 25, 2018 and may not reflect all publicly available security updates. See configuration disclosure for details. No component or product can be absolutely secure.

BACKUP

Performance Results (From X17)



2 x Intel® Xeon® Gold 6152 Processor H0 @ 2.1 GHz, Intel C627 Chipset B1, x16+x8 PCI lanes, DDR4 2400 MHz 16 GB

22 cores used for Nginx* tasks

1. Results have been estimated based on internal Intel analysis and are provided for informational purposes only. Any difference in system hardware or software design or configuration may affect actual performance.
2. All products, platforms, dates, features, and figures specified are preliminary based on current expectations and are subject to change without notice.
3. Software and workloads used in performance tests may have been optimized for performance only on Intel microprocessors.

   Performance tests, such as SYSmark* and MobileMark*, are measured using specific computer systems, components, software, operations and functions. Any change to any of those factors may cause the results to vary. You should consult other information and performance tests to assist you in fully evaluating your contemplated purchases, including the performance of that product when combined with other products. For more complete information visit www.intel.com/benchmarks.

   Configurations: See slide 9 and 10 for configuration. Testing performed by Intel.
4. Performance results are based on testing as of September 1, 2017 and may not reflect all publicly available security updates. See configuration disclosure for details. No component or product can be absolutely secure.

Acknowledgments

Acknowledgments

- Mark Chambers, Joel Schuetze, Jon Strang

Thank you

Gordon.mcfadden@intel.com